Docket No. 244696US2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Motokazu KAWAKI GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: CONTENTS REPRODUCING APPARATUS, CONTENTS REPRODUCTION CONTROL PROGRAM AND RECORDING MEDIUM HAVING A CONTENTS REPRODUCTION CONTROL PROGRAM RECORDED THEREON

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-333546	November 18, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１１月１８日

出願番号
Application Number: 特願２００２－３３３５４６

[ST.10/C]: [ＪＰ２００２－３３３５４６]

出願人
Applicant(s): 三菱電機株式会社

２００３年　６月１３日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４６４３５

【書類名】　特許願
【整理番号】　543128JP01
【提出日】　平成14年11月18日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/60
G06F 13/00
【発明者】
【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
【氏名】　河木　理一
【特許出願人】
【識別番号】　000006013
【氏名又は名称】　三菱電機株式会社
【代理人】
【識別番号】　100102439
【弁理士】
【氏名又は名称】　宮田　金雄
【選任した代理人】
【識別番号】　100092462
【弁理士】
【氏名又は名称】　高瀬　彌平
【手数料の表示】
【予納台帳番号】　011394
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えたことを特徴とするコンテンツ再生装置。

【請求項２】　前記コンテンツ再生制御手段により起動され、前記コンテンツデータの利用制限情報に従って入力手段から入力される操作信号を無効にする利用制限制御手段を設けたことを特徴とする請求項１に記載のコンテンツ再生装置。

【請求項３】　ネットワークに接続するインターフェース部が設けられ、前記ネットワークに接続したサーバ装置から前記暗号化データを取得するようにしたことを特徴とする請求項１記載のコンテンツ再生装置。

【請求項４】　媒体読取手段が設けられ、この媒体読取手段により記録媒体に記録された前記暗号化データを取得するようにしたことを特徴とする請求項１記載のコンテンツ再生装置。

【請求項５】　保存手段に保存された暗号化データを取得し、この暗号化データから復元したコンテンツデータにより再生したイメージデータをブラウザのブラウザ画面上に表示させるコンピュータに、入力手段から入力された識別情報に基づき前記ブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ

及びその利用制限情報を一時的に記憶手段に記憶する記憶処理と、前記コンテンツデータの利用制限情報に応じて前記ブラウザ画面上にブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とを実現させることを特徴とするコンテンツ再生制御プログラム。

【請求項６】　保存手段に保存された暗号化データを取得する処理と、入力手段から入力された識別情報と予め記憶した識別情報とを照合して前記識別情報を入力した利用者の使用許可又は不許可を判別する認証処理と、前記認証処理の判別結果に基づいてブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を記憶手段に一時的に記憶する記憶処理と、前記記憶手段に記憶した前記コンテンツデータによりイメージデータを再生して前記ブラウザ画面上に表示させる表示処理と、前記コンテンツデータの利用制限情報に応じてブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とをコンピュータに実現させることを特徴とするコンテンツ再生制御プログラム。

【請求項７】　前記識別情報は、ユーザＩＤとパスワードであることを特徴とする請求項５又は請求項６に記載のコンテンツ再生制御プログラム。

【請求項８】　前記利用制限情報は、利用者毎に登録された複数の利用制限情報であることを特徴とする請求項５又は請求項６に記載のコンテンツ再生制御プログラム。

【請求項９】　請求項５又は請求項６に記載のコンテンツ再生制御プログラムを記録したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、インターネット、イントラネット等の電気通信回線、ＣＤ－ＲＯＭ等の記憶媒体により配布されるデジタルコンテンツ（文字、画像あるいは動画等）をブラウザのブラウザ画面上に表示して閲覧する際に、このブラウザ画面上

に表示されたこれらデジタルコンテンツの印刷、保存等の利用を制限し、利用者による不正利用ないし第三者への情報漏洩を防止するコンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記憶した記録媒体に関する。

【０００２】

【従来の技術】

近年、インターネットの利用者が急増し、インターネットは情報流通あるいはサービス提供のインフラとして不可欠な存在となりつつある。例えば、これまではＣＤ－ＲＯＭ、書籍等の有体物として流通していたコンピュータプログラムや書籍等のいわゆる情報財はパソコンや携帯電話等をつなぐネットワーク上で流通するようになっており、さらにオンラインゲームや電子掲示板の提供等の各種サービスも生まれている。

【０００３】

一方、このようなインターネットの普及に伴い、ネットワークの中を流通する情報の改ざんや不正利用等が行われる危険性も同時に増加しており、今後、プログラム、画像コンテンツ等の流通を普及・促進するためにはこのようなネットワーク内を流通し、パソコン等において表示される情報の不正利用や改ざんを防止するための対策が不可欠となっている。

【０００４】

例えば、このような不正利用を防止する技術として、Ｄｉｇｉｔａｌ・Ｒｉｇｈｔｓ・Ｍａｎｅｇｉｍｅｎｔ（以下、単にＤＲＭという。）と呼ばれる技術がある。このＤＲＭ技術は、どういう利用ができるかの著作権情報とコンテンツとを暗号化して送信し、条件に合致した利用者のみが当該暗号を解読してコンテンツの内容を視聴できるようにするという技術であり、暗号化された条件の設定により、コンテンツを再生できる回数、コンテンツを視聴できる期間、ＣＤやＤＶＤへの保存の可否等を任意に設定することが可能である。

【０００５】

なお、パソコン等の端末装置おいて受信された画像コンテンツ、例えばＷｅｂページ等はブラウザを用いて表示させるのが一般的である。このＷｅｂブラウザ

は、Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（以下、ＵＲＬという。）によって指定されたＷｅｂコンテンツの要求とこれらの表示を実行するためのアプリケーション・プログラムであり、ハイパーテキスト転送プロトコル（以下、ＨＴＭＬという）の要求の中でＵＲＬを指定する。この要求はＵＲＬによって指定された情報やコンテンツをサポートするＷｅｂサーバ装置に転送され、対応するコンテンツがＷｅｂサーバ装置から要求のあった端末装置に対して送信される。

【０００６】

【特許文献１】

特開２００２－２２９４４７公報（第４頁左欄第２９行目乃至同頁右欄第５行目の記載事項を参照。）

【０００７】

【発明が解決しようとする課題】

しかしながら、従来のＷｅｂブラウザ等のアプリケーション・プログラムは、文字、画像コンテンツ等の公開を念頭に設計されているため、パソコン等のブラウザ画面上に表示された後のコンテンツはブラウザの印刷機能やファイル保存機能等によってＷｅｂサイト利用者の手元に簡単に保存することができるよう構成されており、たとえ暗号化されたデジタルコンテンツを配信するように構成されていても、暗号化データを復号化するのみで表示後のデジタルコンテンツの利用を制限する配慮が何らなされていない場合には、これら表示後のデジタルコンテンツが利用者により不正に利用され、容易に漏洩してしまうという問題点があった。

【０００８】

これに対し、閲覧のみを許可して印刷やファイル保存等は許可しないようにするという機能をブラウザの機能として付加することも可能であるが、そのためにはそのような機能を有する新規なＷｅｂブラウザを作成しなければならず、また、一般に公開されているＷｅｂブラウザを利用する場合には無断でそのような機能を設けることはできない等の問題点があった。

【０００９】

また、ＤＲＭ技術を使用する場合には、コンテンツの配信を行うサーバ装置とは別に著作権情報管理サーバと呼ばれる専用のサーバ装置を設ける必要があり、課金に応じたコンテンツの視聴等、様々なビジネスモデルに対応する条件設定が可能となる一方、このような特別のサーバ装置を設置しなければならないというシステム上の問題点がある。

【００１０】

この発明は上記のような課題を解消するためになされたもので、特別のサーバ装置等を設けることなく、また、一般に公開されているブラウザを利用したままで当該ブラウザ画面上に表示されたデジタルコンテンツの不正利用ないし第三者への漏洩を防止することができる新規なコンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記録した記録媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】

請求項１の発明に係るコンテンツ再生装置は、暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えたものである。

【００１２】

請求項２の発明に係るコンテンツ再生装置は、前記コンテンツ再生制御手段により起動され、前記コンテンツデータの利用制限情報に従って入力手段から入力される操作信号を無効にする利用制限制御手段を設けたものである。

【００１３】

請求項３の発明に係るコンテンツ再生装置は、ネットワークに接続するインターフェース部が設けられ、前記ネットワークに接続したサーバ装置から前記暗号化データを取得するようにしたものである。

【００１４】

請求項４の発明に係るコンテンツ再生装置は、媒体読取手段が設けられ、この媒体読取手段により記録媒体に記録された前記暗号化データを取得するようにしたものである。

【００１５】

請求項５の発明に係るコンテンツ再生制御プログラムは、保存手段に保存された暗号化データを取得し、この暗号化データから復元したコンテンツデータにより再生したイメージデータをブラウザのブラウザ画面上に表示させるコンピュータに、入力手段から入力された識別情報に基づき前記ブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶手段に記憶する記憶処理と、前記コンテンツデータの利用制限情報に応じて前記ブラウザ画面上にブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とを実現させるものである。

【００１６】

請求項６の発明に係るコンテンツ再生制御プログラムは、保存手段に保存された暗号化データを取得する処理と、入力手段から入力された識別情報と予め記憶した識別情報とを照合して前記識別情報を入力した利用者の使用許可又は不許可を判別する認証処理と、前記認証処理の判別結果に基づいてブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を記憶手段に一時的に記憶する記憶処理と、前記記憶手段に記憶した前記コンテンツデータによりイメージデータを再生して前記ブラウザ画面上に表示させる表示処理と、前記コンテンツデータの利用制限情報に応じてブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブ

ラウザ補助機能処理とをコンピュータに実現させるものである。

【００１７】

請求項７の発明に係るコンテンツ再生制御プログラムは、前記識別情報がユーザＩＤとパスワードであるものである。

【００１８】

請求項６の発明に係るコンテンツ再生制御プログラムは、利用者毎に登録された複数の利用制限情報であるものである。

【００１９】

請求項９の発明に係るプログラム記録媒体は、請求項５又は請求項６に記載のコンテンツ再生制御プログラムを記録したことを特徴とするものである。

【００２０】

【発明の実施の形態】

実施の形態１.

以下、この発明の実施の形態１について図１乃至図６を用いて説明する。図１は実施の形態１によるコンテンツ再生方法を実現するためのシステム構成図、図２はコンテンツ再生装置等の具体的構成を示す機能ブロック図である。図１及び図２において、１はＷｅｂコンテンツのコンテンツデータを保存するＷｅｂサーバー装置（以下、サーバ装置という。）、２はインターネット、イントラネット等の電気通信回線（以下、ネットワークという。）、３はネットワーク２を介してサーバー装置１と接続したパソコン、携帯情報端末（ＰＤＡ）等であって、表示部８に生成されたブラウザ画面上にコンテンツデータにより再生したイメージデータ、すなわちＷｅｂコンテンツを表示するコンテンツ再生装置である。

【００２１】

サーバ装置１には所定の暗号方式を用いて暗号化されたＷｅｂコンテンツのコンテンツデータ及びその利用制限情報が保存されており（以下、暗号化データという。）、実施の形態１によるコンテンツ再生装置（以下、端末装置という。）３により閲覧する各Ｗｅｂコンテンツはサーバ装置１からネットワーク２を介して端末装置３に配信（ダウンロード）される。Ｗｅｂコンテンツの種類としては、いわゆるＨＴＭＬファイル、各種画像ファイル（ＢＭＰ形式、ＧＩＦ形式、Ｊ

ＰＥＧ形式、ＰＮＧ形式等）、ＰＤＦファイル等があり、各コンテンツ毎に対応する利用制限情報が付加されている。

【００２２】

また、端末装置３にはサーバ装置１からダウンロードした暗号化データを格納する暗号化データ格納部４、利用制限制御プログラムを格納する利用制限制御ライブラリ格納部５、コンテンツ再生制御プログラムを格納するコンテンツ再生制御プログラム格納部６、Ｗｅｂブラウザプログラムを格納するＷｅｂブラウザ格納部７、及び復号化処理により復元されたコンテンツデータにより再生されたＷｅｂコンテンツを表示するブラウザ画面が生成される表示部がそれぞれ設けられており、サーバ装置１から配信された暗号化データは端末装置３に設けられたネットワーク２とのインタフェース部（図示省略する。）を介して暗号化データ格納部４に格納される。

【００２３】

なお、実施の形態１によるコンテンツ再生装置においては、コンテンツ再生制御プログラムもサーバ装置１に保存されており、端末装置３の転送要求に応じてサーバ装置１からネットワーク２を介して端末装置３に配信される。端末装置３に配信されたコンテンツ再生制御プログラムはインタフェース部を介してコンテンツ再生制御プログラム格納部６に格納される。

【００２４】

ここで、暗号化データ格納部４、利用制限制御ライブラリ格納部５、及びＷｅｂブラウザ格納部７は、端末装置３内のハードディスク等の物理的記憶媒体上にそれぞれ設けているが、コンテンツ再生制御プログラム格納部６は、端末装置３内のデータを一時的に記憶する電子部品、例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等のメモリ上に設けている。すなわち、この発明に係るコンテンツ再生制御プログラムは、ＲＡＭ等のメモリ内に格納され、このようなメモリ上で動的に生成させるものである。

【００２５】

また、図２において、９，１０はそれぞれサーバ装置１内に保存され端末装置３にダウンロードされるコンテンツ再生制御プログラム及び暗号化データ、１１

はサーバ装置１からコンテンツ再生制御プログラム９をダウンロードするために起動される呼び出し用ＨＴＭＬ部である。この呼び出し用ＨＴＭＬ部１１は、Ｗｅｂブラウザ格納部７に格納されたＷｅｂブラウザが起動して表示部８にブラウザ画面が生成されるとそのブラウザ画面上に表示される。端末装置３の利用者はブラウザ画面上に表示された呼び出し用ＨＴＭＬ部１１にアクセスすることによりサーバ装置１に対するコンテンツ再生制御プログラム９の転送要求を行うことができる。

【００２６】

また、１２はＷｅｂブラウザ格納部７において起動され、ＨＴＭＬで記述された一般のＷｅｂコンテンツの解読・表示等を行うＷｅｂブラウザプログラム（以下、Ｗｅｂブラウザという。）、１３，１４はコンテンツ再生制御プログラム格納部６において起動されるコンテンツ再生制御プログラム９を構成するライブラリ制御部及び認証部であり、ライブラリ制御部１３は認証部１４及び利用制限制御ライブラリ格納部５において起動する利用制限制御ライブラリを構成するキー制御ライブラリ１５の起動を制御する。また、認証部１４は表示部８のブラウザ画面上に識別情報、例えば、ユーザＩＤとパスワードの入力を促す認証画面を生成して端末装置３の利用者に識別情報の入力を求める処理を行う。認証画面内に入力された識別情報と予め記憶した識別情報とが一致すれば、キー制御ライブラリ１５にその旨の認証情報を通知する一方、その識別情報を入力した利用者に対してコンテンツ再生制御プログラム９の利用が可能であることを知らせるメッセージをブラウザ画面上に表示する。

【００２７】

また、１５，１６及び１７は利用制限制御ライブラリ格納部５において起動される利用制限制御ライブラリを構成するキー制御ライブラリ、インスタンス管理ライブラリ及び復号化ライブラリであり、キー制御ライブラリ１５は認証部１４からの認証情報、及び復号化処理により復元されたコンテンツデータの利用制限情報に基づきブラウザ１２のコンテンツ利用機能の利用制限処理を実行する。インスタンス管理ライブラリ１６はキー制御ライブラリ１５からの指示により起動され、ブラウザ１２の起動状態を確認し、復号化ライブラリ１７は暗号化データ

格納部４に格納された暗号化データ１０を復号化処理して元のコンテンツデータ及びその利用制限情報を復元する。

【００２８】

また、１８は復号化ライブラリ１７の復号化処理により復元されコンテンツ再生制御プログラム格納部６に一時的に記憶された平文のコンテンツデータ（以下、平文コンテンツという。）、１９は同様に復号化ライブラリ１７の復号化処理により復元されコンテンツ再生制御プログラム格納部６に一時的に記憶された平文コンテンツ１８の利用制限情報、２０はコンテンツ再生制御プログラム９の制御により利用不可となったブラウザ１２のコンテンツ利用機能に相当するブラウザ補助機能を表示部８のブラウザ画面上に生成し、利用制限情報１９に従って当該機能の操作を利用者に促すブラウザ補助機能プログラム（以下、ブラウザ補助機能という。）、２１は平文コンテンツ１８からイメージデータを再生して表示部８のブラウザ画面上に表示する処理を行う表示処理部である。

【００２９】

なお、図３は端末装置３に配信される暗号化データ１０のデータ構成を示すデータ構成図である。図３において平文コンテンツ１８及びその利用制限情報１９は所定の所定の暗号方式によって暗号化された状態を示しており、図３に示すように、暗号化データ１０は所定の暗号方式によって暗号化された平文コンテンツ１８及び利用制限情報１９を一体化することにより生成している。そして、このような使用制限情報１９が平文コンテンツ１８と併せて復元されることにより利用者による不正利用、第三者への情報の漏洩を防止している。この平文コンテンツ１８及び利用制限情報１９には異なる暗号方式を使用することができる。例えば、平文コンテンツ１８は鍵Ａ、利用制限情報１９は別の鍵Ｂを用いて暗号化することができ、異なる暗号方式を使用することにより端末装置３に配信されるまでのネットワーク２内における情報の漏洩、改ざん等を確実に防止することができる。

【００３０】

また、図３に示すように、利用制限情報１９は利用者毎に登録することができる。例えば、利用者Ａには平文コンテンツ１８に基づきブラウザ画面上に表示さ

れたＷｅｂコンテンツの印刷のみを許可する利用制限情報Ａ、利用者Ｂには平文コンテンツ１８に基づきブラウザ画面上に表示されたＷｅｂコンテンツの印刷及びファイル保存を許可する利用制限情報Ｂ等を登録することができる。このように、一つの平文コンテンツ１８に対して複数の利用制限情報（Ａ，Ｂ，Ｃ，…）を登録することができるので、共通の暗号化データ１０を多数の利用者によって利用することができる。

【００３１】

次に、動作について図４及び図５を用いて説明する。図４は図１に示す端末装置３の一連の処理について説明するためのフローチャート図、図５は端末装置３の利用制限処理について説明するためのフローチャート図である。端末装置３の利用者がサーバ装置１に保存された暗号化データ１０を取得してその中のＷｅｂコンテンツの閲覧を行う場合、利用者はまずマウス、キーボード等の入力手段を介して所定のブラウザ１２を起動する（Ｓ０１）。

【００３２】

ブラウザ１２が起動すると、表示部８にブラウザ１２のブラウザ画面が生成され、そのブラウザ画面上に呼び出し用ＨＴＭＬ部１１が生成される。利用者は呼び出し用ＨＴＭＬ部１１に表示された呼び出し用ＨＴＭＬにアクセスすることによりサーバ装置１に対するコンテンツ再生制御プログラム９の転送要求を行う（Ｓ０２）。サーバ装置１は呼び出し用ＨＴＭＬ部１１によるコンテンツ再生制御プログラム９の転送要求が行われると、この転送要求を行った端末装置、ここでは端末装置３に対してコンテンツ再生制御プログラム９を配信（ダウンロード）する。コンテンツ再生制御プログラム９はネットワーク２介してダウンロードされ端末装置３に設けられたインタフェース部を介してコンテンツ再生制御プログラム格納部６内に格納される（Ｓ０２）。

【００３３】

サーバ装置１からダウンロードされたコンテンツ再生制御プログラム９がコンテンツ再生制御プログラム格納部６内に格納されると、コンテンツ再生制御プログラム９は起動してコンテンツ再生制御処理を開始する（Ｓ０３）。

【００３４】

コンテンツ再生制御プログラム９が起動すると、サーバ装置１に保存された暗号化データ１０がネットワーク２を介してダウンロードされ、端末装置３内の暗号化データ格納先４に保存される（Ｓ０４）。

【００３５】

暗号化データ格納先４に暗号化データ１０が保存されると、コンテンツ再生制御プログラム９のライブラリ制御部１３が起動して認証部１４による認証処理を起動させる（Ｓ０５）。

【００３６】

認証部１４は、認証用のダイアログボックス、すなわちユーザＩＤ、パスワード等の識別情報（以下、識別情報という。）を入力するための認証画面をブラウザ１２のブラウザ画面上に生成させ利用者に識別情報の入力を促す。利用者が入力した識別情報と予め記憶した識別情報とが一致しない場合は、暗号化データ格納先４に保存されている暗号化データ１０がその利用者によって閲覧できる暗号化データではないと判断しその後の処理を行わずに処理を終了する。一方、利用者が入力したユーザＩＤ、パスワードと予め記憶した識別情報とが一致した場合は、認証成功と判断する（Ｓ０６）。

【００３７】

認証部１４により利用者が入力した識別情報と予め記憶した識別情報とが一致すると判断されると、ライブラリ制御部１３が利用制限制御ライブラリ格納部５内のキー制御ライブラリ１５を起動して、ブラウザ機能制限処理を実行する一方、認証部１４の認証情報がキー制御ライブラリ１５に通知される（Ｓ０７）。

【００３８】

キー制御ライブラリ１５は、ブラウザ１２の種類及びバージョンがコンテンツ再生制御プログラム９が許可しているか否かを判別し、許可されていないブラウザであると認識した場合はその後の処理を行わずに終了する処理を行う（Ｓ０８）。判別の結果、許可されているブラウザであると認識した場合はインスタンス管理ライブラリ１６を起動してブラウザ１２の起動が継続しているか否かの監視処理を実行する（Ｓ０９）。

【００３９】

また、キー制御ライブラリ１５は、ブラウザ機能制限処理が継続している間、機能制御ライブラリ格納部５内の復号化ライブラリ１７を起動して暗号化データ格納部４内に保存された暗号化データ１０の復号化処理を実行する。この復号化ライブラリ１７による復号化処理により暗号化データ格納部４内に保存された暗号化データ１０から平文コンテンツ１８及び対応する利用制限情報１９がそれぞれ復元される。ここで、暗号化データ１０は利用者毎に設定した複数の利用制限情報を含んでおり、認証部１４において認証成功と判断された識別情報と一致する識別情報を有する利用制限情報、例えば利用者Ａであれば利用制限情報Ａが復号化ライブラリ１７により復元される。この復元された平文コンテンツ１８及び利用制限情報Ａはコンテンツ再生制御プログラム格納部６内に保存される（Ｓ１０）。

【００４０】

キー制御ライブラリ１５は、復元された利用制限情報Ａから当該利用者に対して許可されたブラウザ１２のコンテンツ利用機能の有無を判断し（Ｓ１１）、許可された機能があればその機能の実行にあたるキー入力の監視を解除する処理を行う（Ｓ１２）。一方、コンテンツ再生制御プログラム１０は、利用制限情報１９に登録された利用制限規則から当該利用者に対して許可されたコンテンツ利用機能の有無を判断し、許可された機能があればブラウザ補助機能２０として表示部８のブラウザ画面上に生成する（Ｓ１３）。各利用者はブラウザ画面上に表示されたブラウザ補助機能２０を利用することによりブラウザ画面上に表示されたＷｅｂコンテンツを利用することができ、このブラウザ補助機能２０を利用してブラウザ画面上に表示されたＷｅｂコンテンツの印刷、保存等を行う。

【００４１】

このように、復号化ライブラリ１７の復号化処理によって暗号化データ１０から平文コンテンツ１８及び利用者の識別情報に一致する利用制限情報、例えば利用制限情報Ａがそれぞれ復元され（Ｓ１４）、復元された平文コンテンツ１８については表示処理部２１がその平文コンテンツ１８に基づきイメージデータ、すなわちＷｅｂコンテンツを再生し表示部８のブラウザ画面上に表示する（Ｓ１５）。

【００４２】

この際、平文コンテンツ１８及び利用制限情報１９はすべてコンテンツ再生制御プログラム格納部６、すなわち端末装置３内に設けられたＲＡＭ等のメモリ上のみで管理されるので、これら平文コンテンツ１８及び利用制限情報１９が端末装置３内のハードディスクやキャッシュ等に残らず、情報の漏洩を防止することができ、ブラウザ画面上に表示されたコンテンツの安全性が保証される。

【００４３】

このように、サーバ装置１からダウンロードされる暗号化データ１０には、Ｗｅｂコンテンツを再生するための平文コンテンツ１８とこの平文コンテンツ１８に再生されたＷｅｂコンテンツを閲覧する際の利用制限規則を記述した利用制限情報１９とが含まれているので、各利用者は、識別情報（ユーザＩＤとパスワード等）の一致する利用制限情報１９に記述された利用制限規則に従って平文コンテンツ１８の利用を行うことができる。すなわち、Ｗｅｂコンテンツの配信側は各利用者に応じた複数の利用制限情報１９と平文コンテンツ１８とからなる暗号化データ１０をサーバ装置１に保存しておき、各利用者は自分の識別情報に一致する利用制限情報１９に記述された利用制限規則に従って平文コンテンツ１８の利用ができるように構成することにより、特別なサーバ装置等を設けることなく特定の利用者のみが平文コンテンツ１８に基づくＷｅｂコンテンツの閲覧ないし利用を行うことができる。

【００４４】

例えば、利用者Ａに対応する利用制限情報Ａにブラウザ１２の印刷機能のみを許可する利用制限規則が登録されていれば、表示部８のブラウザ画面上にはブラウザ１２の印刷機能の利用を促すブラウザ補助機能２０が生成され、利用者Ａは当該印刷機能によりブラウザ画面上に生成された平文コンテンツ１８の印刷を行うことができる。また、利用者Ｂに対応する利用制限情報Ｂにブラウザ１２の印刷機能及び画面コピーを許可する利用制限規則が登録されていれば、表示部８のブラウザ画面上にはブラウザ１２の印刷機能及び画面コピーの利用を促すブラウザ補助機能２０が表示され、利用者Ｂは当該印刷機能及び画面コピー機能によりブラウザ画面上に表示された平文コンテンツ１８の印刷、画面コピーを行うこと

ができる。

【００４５】

なお、利用制限情報１９に登録する利用制限規則としては、ブラウザ画面に表示されたイメージデータの印刷許可する印刷許可、保存を許可する保存許可、画面コピーを許可各する画面コピー許可等がある。また、印刷許可、保存許可等の回数、さらにはイメージデータを再生して閲覧することができる閲覧回数及び閲覧期間等についても利用制限規則として登録することができる。

【００４６】

次に、コンテンツ再生装置３の利用制限処理について図４を用いて詳細に説明する。利用制限処理とは、ブラウザ１２の判別、起動状態を監視する処理を行う一方、コンテンツ再生制御プログラム１０の起動により使用禁止となったブラウザ１２のコンテンツ利用機能を暗号化データ１０に含まれた利用制限情報１９に基づいて利用者に許可する処理である。起動しているブラウザ１２の種類とバージョンはキー制御ライブラリ１５によって判別する（Ｓ０１）。コンテンツ再生制御プログラム１０が許可していないブラウザである判断した場合は、復号化の処理を中断する指示をコンテンツ再生制御プログラム１０に与えてその後の復号化に関する処理を行わずに終了する（Ｓ０２，Ｓ０３）。

【００４７】

ブラウザ１２の起動状態の監視はキー制御ライブラリ１５に起動されたインスタンス管理ライブラリ１６により行う（Ｓ０４）。ブラウザ１２が終了していると判断した場合は、インスタンス管理ライブラリ１６からキー制御ライブラリ１５に対してその後の処理を終了する指示が与えられ、キー制御ライブラリ１５はコンテンツ再生制御プログラム１０の起動により使用禁止としたブラウザ１２に対するキー制御を開放する（Ｓ０５，Ｓ０６）。

【００４８】

インスタンス管理ライブラリ１６がブラウザ１２が起動していると判断した場合は、キー制御ライブラリ１５はブラウザ機能制限処理を継続し、端末装置３に接続されたキーボード等の入力手段（図示省略する。）からのイベントをハンドリングする（Ｓ０７）。具体的には、入力手段から印刷実行、画面コピー等のキ

ー入力がされた場合に（Ｓ０８）、そのキー入力が利用者毎に設定されたコンテンツ利用制限情報１９を考慮して管理対象、すなわち使用許可されていない操作であるか否かを判断し（Ｓ０９）、管理対象であると判断した場合はそのキー入力を無効化する（Ｓ１０）。

【００４９】

以上の処理はブラウザ１２の起動が終了するまで継続され、その間における入力手段からのキー入力が暗号化データ１０から読み出された利用制限情報１９に基づいて利用制限される。

【００５０】

図６はコンテンツ再生制御プログラム９の起動により表示部８のブラウザ画面上に生成されたコンテンツ再生制御プログラム９のインタフェース画面等を示す表示画面図である。図６において、２２はコンテンツ再生制御プログラム９により無効化されたブラウザ１２の表示メニュー（コンテンツ利用機能）、２３はブラウザ補助機能２０内に生成された印刷機能である。通常、ブラウザ画面に表示されたＷｅｂコンテンツの内容はブラウザ１２の表示メニューを操作して印刷、保存等することが可能であるが、無効化された表示メニュー２２に対するマウス、キーボードによる操作はキー制御ライブラリ１５の無効化処理により一切受け付けられないので、端末装置３の利用者はこの無効化された表示メニュー２２を通しての印刷や保存等の操作を行うことはできない。しかし、識別情報の一致した利用者は暗号化データ１０から復元された利用制限情報１９に基づいてブラウザ画面上にブラウザ補助機能２０が生成されるので、このブラウザ補助機能２０を介して許可された機能、例えば印刷機能２３等を操作してブラウザ画面上に表示されたＷｅｂコンテンツの印刷、保存、画面コピー等を行うことができる。

【００５１】

以上のように、実施の形態１による端末装置３においては、Ｗｅｂコンテンツを表示するブラウザ１２のコンテンツ利用機能がコンテンツ再生制御プログラム９によって使用禁止にされる一方、このコンテンツ利用機能に代わるブラウザ補助機能２０を生成して特定の利用者のみがブラウザ画面上に表示されたＷｅｂコンテンツを利用できるようにしたので、第三者による不正利用を確実に防止する

ことができる。また、ブラウザ補助機能２０は利用者毎に登録した利用制限情報１９に従って生成されるので、各利用者は識別情報の一致した利用制限情報１９により許可されたブラウザ補助機能２０しか利用することができず、コンテンツの利用が許可れた利用者による不正利用をも防止することができ、ブラウザ画面上に表示されたＷｅｂコンテンツの漏洩を確実に防止することができる。

【００５２】

また、復号化ライブラリ１の復号化処理により復元された平文コンテンツ１８及び利用制限情報１９はすべてコンテンツ再生制御プログラム格納部６、すなわち端末装置３内に設けられたＲＡＭ等のメモリ上のみで管理されるので、Ｗｅｂコンテンツが表示された後はこれら平文コンテンツ１８及び利用制限情報１９が端末装置３内のハードディスクやキャッシュ等に残らず、この点においてもＷｅｂコンテンツの漏洩を確実に防止することができる。

【００５３】

また、コンテンツ再生制御プログラム９は、Ｗｅｂブラウザと連携して起動する機械依存のないプログラムであり、ブラウザ１２上で当該プログラムを実行するこができるので、一般に公開されている各種のＷｅｂブラウザと連携して使用することができる。これにより、一般に公開されているブラウザと異なる新規なブラウザを作成する必要がない。

【００５４】

なお、以上の説明では利用者の認証に関し、あらかじめ利用者に通知されてあるユーザＩＤ、パスワードを使用するものについて説明したが、別途配布する共通鍵を併用するようにしてもよい。このように共通鍵を併用することで、たとえユーザＩＤ、パスワードが漏洩しても共通鍵が一致しなければ上述したような閲覧を行うことは不可能であり、サーバ装置１から配信されるコンテンツの利用者をより厳密に特定することができる。

【００５５】

実施の形態２．

次に、この発明の実施の形態２について図７及び図８を用いて説明する。図７は実施の形態２によるコンテンツ再生方法を実現するためのシステム概要図、図

２は図１に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。図７及び図８において、２４はＣＤ－ＲＯＭ、ＤＶＤ等の記録媒体、２５はＣＤ－ＲＯＭドライブ、ＤＶＤ－ＲＯＭドライブ等の媒体読取装置であり、実施の形態２によるコンテンツ再生システムでは、暗号化データ１０を保存する手段がネットワーク２に接続されたサーバ装置１ではなく、ＣＤ－ＲＯＭ、ＤＶＤ等の記録媒体２４である。

【００５６】

従って、コンテンツ再生装置３ｂは記録媒体２４からコンテンツ再生制御プログラム９及び暗号化データ１０を取得する必要があり、図７及び図８に示すように記憶媒体２３内に保存されたデータを端末装置３内に読み出すためのＣＤ－ＲＯＭドライブ、ＤＶＤ－ＲＯＭドライブ等の媒体読取装置２５が内蔵もしくは外付けされている。なお、図中、同一符号は同一または相当部分を示し、これらについての詳細な説明は省略する。また、実施の形態２における端末装置３においても図６に示すようなブラウザ画面等が表示される。

【００５７】

実施の形態２においても、利用者が暗号化データ１０を復号化して閲覧する場合は、まずブラウザ１２を起動し、ブラウザ画面上に生成された呼び出し用ＨＴＭＬ部１１によりコンテンツ再生制御プログラム９の転送要求を行う。但し、実施の形態２によるコンテンツ再生装置３ｂにおいては、呼び出し用ＨＴＭＬ部１１の呼び出し用ＨＴＭＬは記憶媒体２４が挿入された媒体読取装置２５を示している。そして、この呼び出し用ＨＴＭＬ部１１にアクセスすることにより記録媒体２４に保存されたコンテンツ再生制御プログラム９への転送要求が実行され、記録媒体２４に保存されたコンテンツ再生制御プログラム媒体読取装置２５を介して端末装置３内のコンテンツ再生制御プログラム格納部６に格納される。なお、以下の動作については実施の形態１とほぼ同様であり説明を省略する。

【００５８】

以上のように、実施の形態２によるコンテンツ再生装置３ｂにおいても、Ｗｅｂコンテンツを表示するブラウザ１２のコンテンツ利用機能がコンテンツ再生制御プログラム９によって使用禁止にされる一方、このコンテンツ利用機能に代わ

るブラウザ補助機能２０を生成して特定の利用者のみがブラウザ画面上に表示されたＷｅｂコンテンツを利用できるようにしたので、第三者による不正利用を確実に防止することができる。また、ブラウザ補助機能２０は利用者毎に登録した利用制限情報１９に従って生成されるので、各利用者は識別情報の一致した利用制限情報１９により許可されたブラウザ補助機能２０しか利用することができず、コンテンツの利用が許可れた利用者による不正利用をも防止することができ、ブラウザ画面上に表示されたＷｅｂコンテンツの漏洩を確実に防止することができる。

【００５９】

また、復号化ライブラリ１７の復号化処理により復元された平文コンテンツ１８及び利用制限情報１９はすべてコンテンツ再生制御プログラム格納部６、すなわち端末装置３ｂ内に設けられたＲＡＭ等のメモリ上のみで管理されるので、これら平文コンテンツ１８及び利用制限情報１９が端末装置３ｂ内のハードディスクやキャッシュ等に残らず、ブラウザ１２の操作によるデジタルコンテンツの漏洩を確実に防止することができる。

【００６０】

【発明の効果】

この発明は、以上説明したように構成されているので、ブラウザ備えている各種のコンテンツ利用機能の使用が半強制的に制限される一方、識別情報の一致した特定の利用者は利用制限情報に基づいてブラウザ画面上に表示されたＷｅｂコンテンツの印刷、保存、画面コピー等を行うことができ、第三者による不正利用を確実に防止することができる。また、各利用者は識別情報の一致した利用制限情報１９により許可されたブラウザ補助機能２０しか利用することができず、コンテンツの利用が許可れた利用者による不正利用をも防止することができ、ブラウザ画面上に表示されたＷｅｂコンテンツの漏洩を確実に防止することができる。これにより、特別のサーバ装置を設けることなく、簡易に情報漏洩の防止を実現することができる。なお、オンラインもしくはオフラインのいずれによって配信されるデジタルコンテンツについても適用することができる。

【００６１】

また、コンテンツ再生制御プログラムは、サーバ装置１又は記憶媒体２３に保存されたコンテンツを閲覧するためのプログラムであるブラウザと連携して起動する機械依存のないプログラムであり、専用のブラウザを新規に作成する必要がなく、既存のブラウザをそのまま使用できる。

【図面の簡単な説明】

【図１】　実施の形態１によるコンテンツ再生方法を実現するためのシステム構成図である。

【図２】　図１に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。

【図３】　コンテンツ再生装置３に配信される暗号化データのデータ構成を示すデータ構成図である。

【図４】　図１に示すコンテンツ再生装置３の一連の処理について説明するためのフローチャート図である。

【図５】　図１に示すコンテンツ再生装置３の利用制限処理について説明するためのフローチャート図である。

【図６】　表示部８のブラウザ画面上に生成されたコンテンツ再生制御プログラム９のインタフェース画面等を示す表示画面図である。

【図７】　実施の形態２によるコンテンツ再生方法を実現するためのシステム構成図である。

【図８】　図１に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。

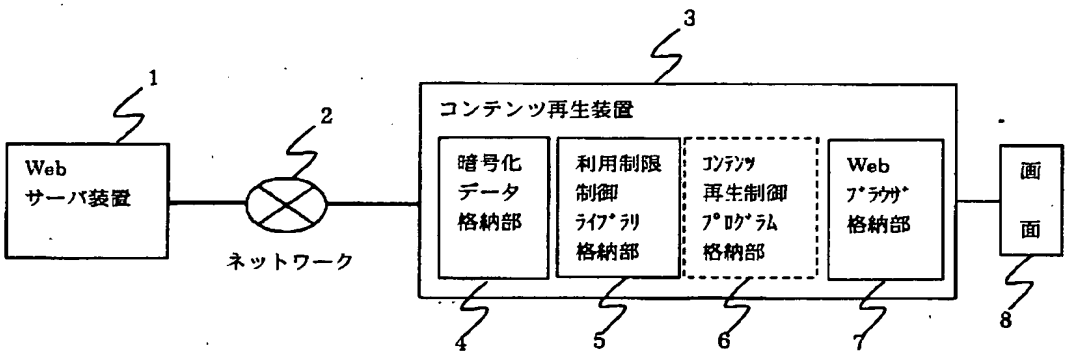
【符号の説明】

１　Ｗｅｂサーバ装置、２　ネットワーク、３，３ｂ　コンテンツ再生装置、
４　暗号化データ格納部、５　利用制限制御ライブラリ格納部、
６　コンテンツ再生制御プログラム格納部、７　Ｗｅｂブラウザ格納部、
８　表示部、９　コンテンツ再生制御プログラム、１０　暗号化データ、
１１　呼び出し用ＨＴＭＬ部、１２　Ｗｅｂブラウザ、
１３　ライブラリ制御部、１４　認証部、１５　キー制御ライブラリ、
１６　インスタンス管理ライブラリ、　１７　復号化ライブラリ、

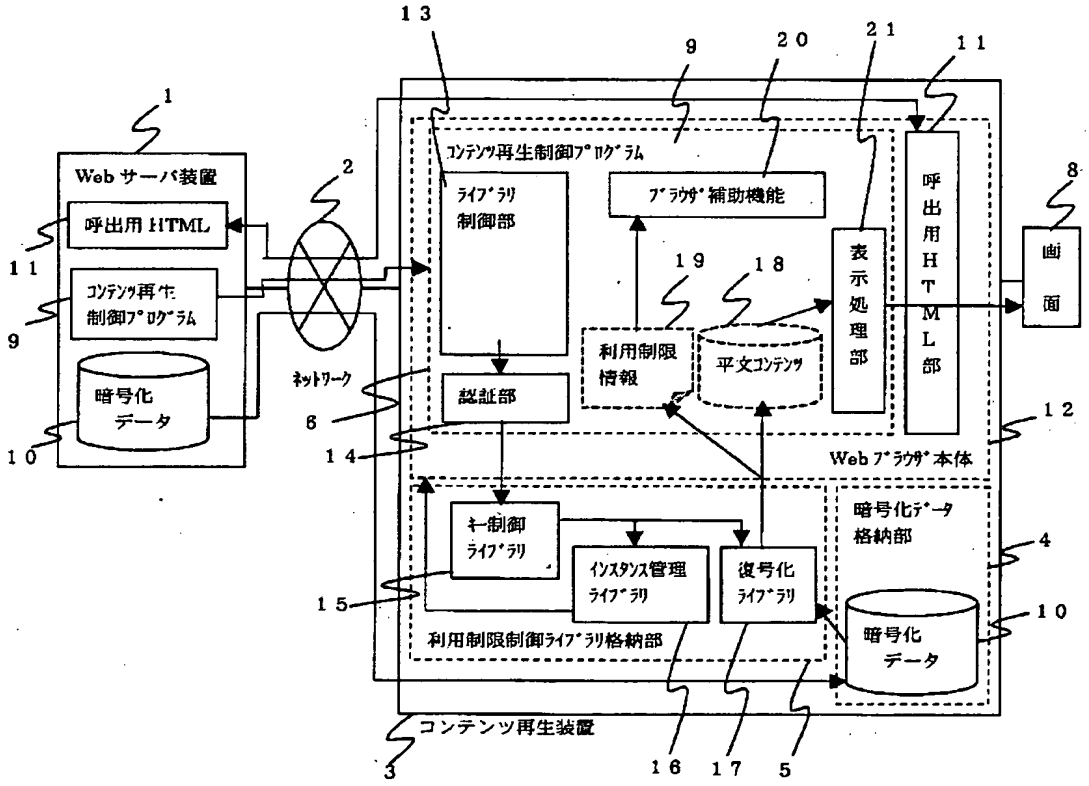
１８　平文のコンテンツデータ、１９　利用制限情報、
２０，２３　ブラウザ補助機能、２１　表示処理部、
２２　無効化されたブラウザの表示メニュー、
２４　記録媒体、　２５　媒体読取装置。

【書類名】　　図面

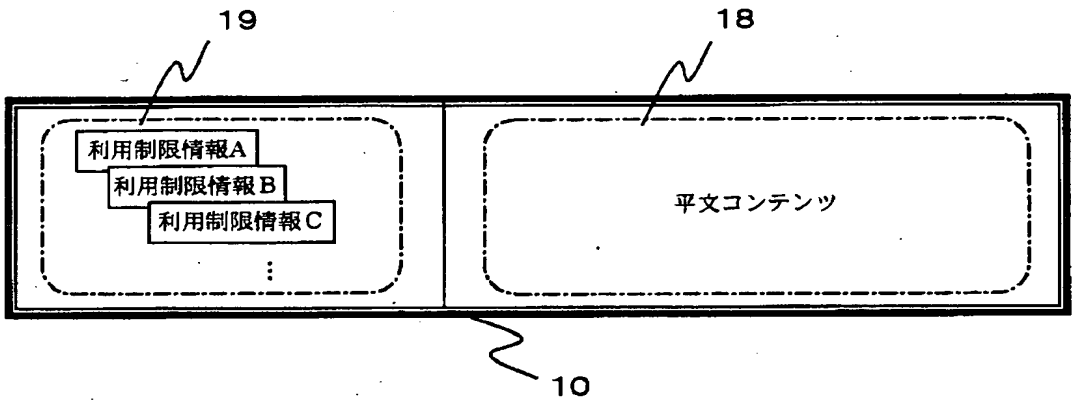
【図１】


1
2
3
Web
サーバ装置
ネットワーク
コンテンツ再生装置
暗号化
データ
格納部
利用制限
制御
ﾗｲﾌﾞﾗﾘ
格納部
ｺﾝﾃﾝﾂ
再生制御
ﾌﾟﾛｸﾞﾗﾑ
格納部
Web
ﾌﾞﾗｳｻﾞ
格納部
画
面
4
5
6
7
8

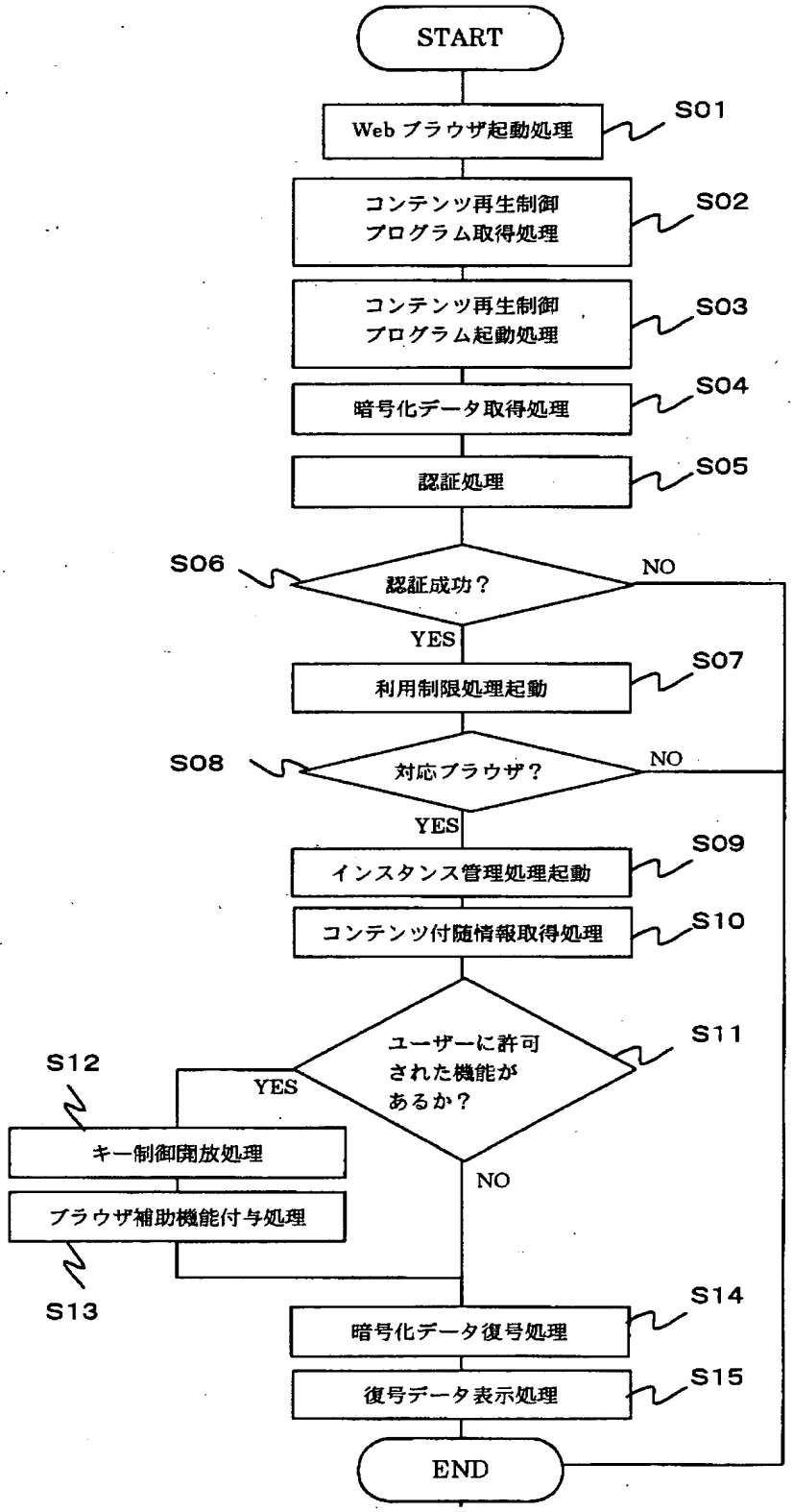
【図２】


13
9
20
21
11
1
Web サーバ装置
呼出用 HTML
11
ｺﾝﾃﾝﾂ再生
制御ﾌﾟﾛｸﾞﾗﾑ
9
暗号化
データ
10
2
ネットワーク
6
14
ｺﾝﾃﾝﾂ再生制御ﾌﾟﾛｸﾞﾗﾑ
ﾗｲﾌﾞﾗﾘ
制御部
認証部
ﾌﾞﾗｳｻﾞ補助機能
19
18
利用制限
情報
平文ｺﾝﾃﾝﾂ
表示
処理
部
呼出用HTML部
8
画面
12
Web ﾌﾞﾗｳｻﾞ本体
暗号化ﾃﾞｰﾀ
格納部
4
10
ｷｰ制御
ﾗｲﾌﾞﾗﾘ
ｲﾝｽﾀﾝｽ管理
ﾗｲﾌﾞﾗﾘ
復号化
ﾗｲﾌﾞﾗﾘ
15
利用制限制御ﾗｲﾌﾞﾗﾘ格納部
暗号化
データ
ｺﾝﾃﾝﾂ再生装置
3
16
17
5

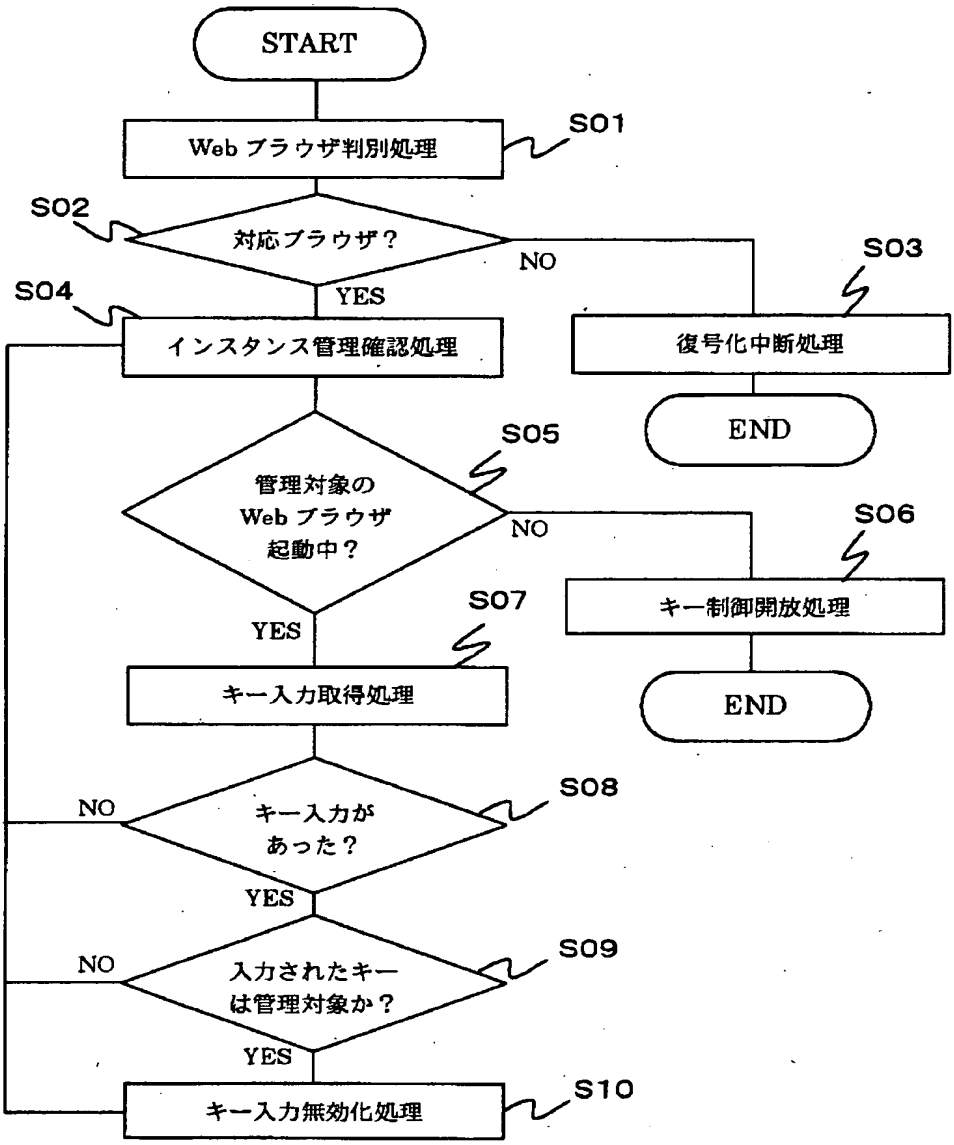
【図３】



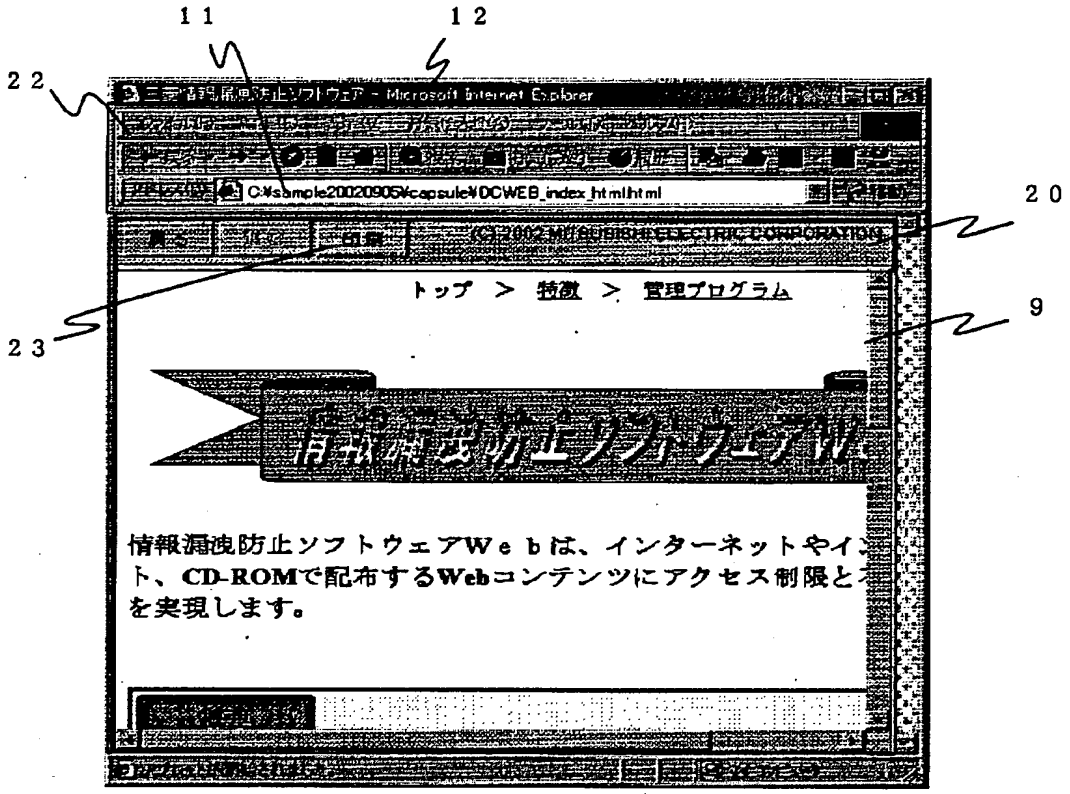
【図４】


START
Web ブラウザ起動処理
S01
コンテンツ再生制御
プログラム取得処理
S02
コンテンツ再生制御
プログラム起動処理
S03
暗号化データ取得処理
S04
認証処理
S05
S06
認証成功？
NO
YES
利用制限処理起動
S07
S08
対応ブラウザ？
NO
YES
インスタンス管理処理起動
S09
コンテンツ付随情報取得処理
S10
ユーザーに許可
された機能が
あるか？
S11
S12
YES
キー制御開放処理
ブラウザ補助機能付与処理
S13
NO
暗号化データ復号処理
S14
復号データ表示処理
S15
END

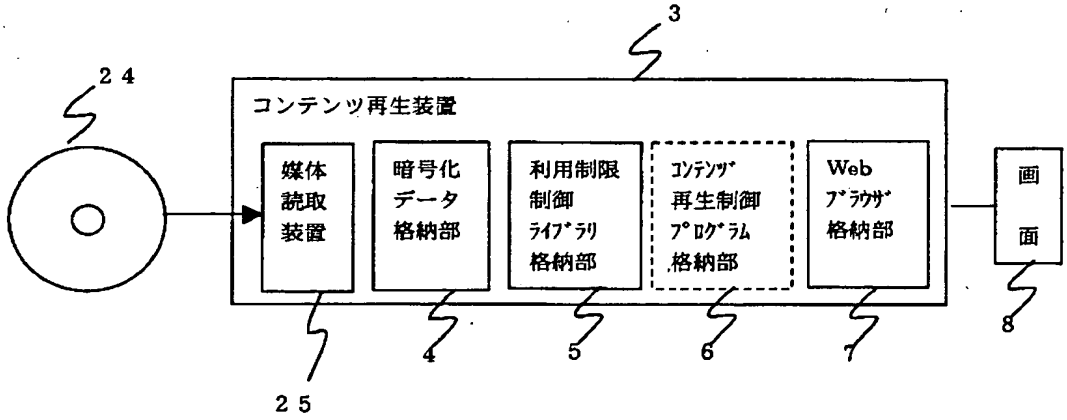
【図５】


START
Web ブラウザ判別処理
S01
対応ブラウザ？
S02
NO
S03
YES
S04
インスタンス管理確認処理
復号化中断処理
END
管理対象の
Web ブラウザ
起動中？
S05
NO
S06
キー制御開放処理
END
YES
S07
キー入力取得処理
キー入力が
あった？
S08
NO
YES
入力されたキー
は管理対象か？
S09
NO
YES
キー入力無効化処理
S10

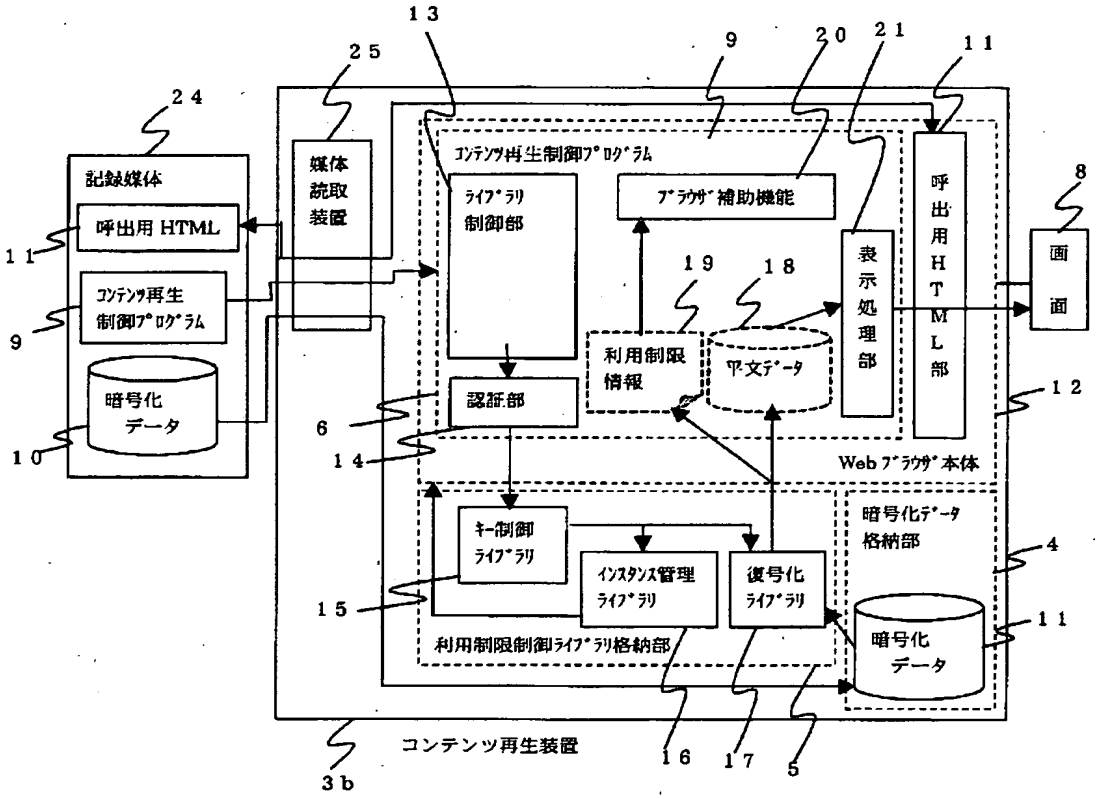
【図６】


11
12
22
20
23
9
トップ ＞ 特徴 ＞ 管理プログラム
情報漏洩防止ソフトウェアＷｅｂは、インターネットやイ
ト、CD-ROMで配布するWebコンテンツにアクセス制限と
を実現します。

【図７】


3
24
コンテンツ再生装置
媒体
読取
装置
暗号化
データ
格納部
利用制限
制御
ﾗｲﾌﾞﾗﾘ
格納部
ｺﾝﾃﾝﾂﾞ
再生制御
ﾌﾟﾛｸﾞﾗﾑ
格納部
Web
ﾌﾞﾗｳｻﾞ
格納部
画
面
25
4
5
6
7
8

【図８】


13
25
9
20
21
11
24
記録媒体
呼出用 HTML
コンテンツ再生制御プログラム
暗号化データ
媒体読取装置
コンテンツ再生制御プログラム
ライブラリ制御部
ブラウザ補助機能
呼出用HTML部
8
画面
19
18
表示処理部
利用制限情報
平文データ
認証部
12
Web ブラウザ本体
暗号化データ格納部
キー制御ライブラリ
インスタンス管理ライブラリ
復号化ライブラリ
利用制限制御ライブラリ格納部
暗号化データ
コンテンツ再生装置
11
10
9
6
14
15
4
16
17
5
3b

【書類名】　　要約書

【要約】

【課題】　特別のサーバ装置等を設けることなく、コンテンツ再生装置において表示したコンテンツの不正利用ないし第三者への情報漏洩を防止する。

【解決手段】　暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えた。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　　東京都千代田区丸の内２丁目２番３号
氏　名　　三菱電機株式会社